PCT WORLD INTELLECTUAL PROPERTY
International Bure

INTERNATIONAL APPLICATION PUBLISHED UNDER T

WO 9605549A1

(51) International Patent Classification 6 : G06F 1/00 — A1

(11) International Publication Number: **WO 96/05549**

(43) International Publication Date: 22 February 1996 (22.02.96)

(21) International Application Number: PCT/US95/08900

(22) International Filing Date: 14 July 1995 (14.07.95)

(30) Priority Data:
08/287,790 9 August 1994 (09.08.94) US

(71) Applicant: SHIVA CORPORATION [US/US]; Northwest Park, 63 Third Avenue, Burlington, MA 01803 (US).

(72) Inventors: HOROWITZ, Michael, Alan; 578 Centre Street, Newton, MA 02158 (US). RODWIN, Andrew, S.; 126 Box Mill Road, Boxborough, MA 01719 (US). WENOCUR, Jonathan, H.; 140 Kilsyth Road, No 4, Brighton, MA 02146 (US).

(74) Agent: TOSTI, Robert, J.; Testa, Hurwitz & Thibeault, High Street Tower, 125 High Street, Boston, MA 02110-2711 (US).

(81) Designated States: AM, AU, BB, BG, BR, BY, CA, CN, CZ, EE, FI, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, TJ, TM, TT, UA, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPARATUS AND METHOD FOR RESTRICTING ACCESS TO A LOCAL COMPUTER NETWORK

(57) Abstract

A remote access server limits access to a local computer network. The server includes at least one communication port for allowing communication with a remote computer and at least one network port for coupling to a local computer network to allow communication with the local computer network. The server also includes processing electronics which control the communication and network ports. The processing electronics also receive a user identification string from the communication port. The string having been entered by a remote user at a remote computer, and it identifies the remote user. The server uses the string to access a database and determine at least one access filter associated with the string. The access filter is used to prevent the remote computer from communicating with at least one predetermined resource on the local computer network. The database includes a user identification string for each remote user and at least one access filter for each user identification string. The server allows the remote computer to access the local computer network and to communicate on the local computer network, but the remote computer is prevented from communicating with the predetermined resource because of the access filter associated with the remote user.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

APPARATUS AND METHOD FOR RESTRICTING ACCESS TO A LOCAL COMPUTER NETWORK

Field of the Invention

This invention relates to an apparatus and method for restricting a remote user's access to a local computer network, and more particularly to a remote access server which restricts the access.

Background of the Invention

The client-server computer networking model allows organizations of all sizes to utilize group productivity products such as e-mail. Many business organizations have grown to rely heavily on network services. Employees who travel typically need to access the same network services and resources provided to them at work. Field offices also frequently need to access the headquarter's network services. The term "telecommuter" has been used to describe an employee who stays at home and conducts business by accessing the network services provided at the traditional worksite. These types of users are sometimes referred to as "remote" because they typically are located in a physically remote place from the networks and because they do not connect to the networks locally or directly. Remote users typically connect to the networks via telephone lines. The terms "remote access" and "remote networking" are used to identify the situation in which a remote user accesses a computer network over analog or digital telephone lines.

A remote user generally can utilize any type of

computer to access the network. The computer can be, for example, a personal computer, a workstation, or a portable computer such as a laptop computer or a notebook computer. Also, the computer can be, for example, an IBM PC or compatible, an Apple Macintosh, or a Unix-based computer. The user typically connects a modem or similar communication device to a serial port of the computer. The modem connected to the user's remote computer communicates over the telephone lines with another modem which is coupled to a server. The other modem and the server are located at the network which the remote computer is attempting to access. The server is coupled directly to the network. It is the server which provides the remote computer with controlled access to the network and the services and resources thereon. The server is referred to as a "remote access server," and it typically includes a serial port for connecting to the other modem, a port for connecting to the network, and electronics which include at least a microprocessor and memory.

It is desirable for the remote access server to have a variety of features. For example, the remote access server should make accessing the network transparent to the remote user. The remote access server also should be easy for a network manager to install and maintain.

Summary of the Invention

It is an object of the invention to provide a remote access server which allows one or more remote computers to access simultaneously a local computer network, even if each of the remote computers employs a different protocol (e.g., IPX, TCP/IP, AppleTalk, NetBEUI, or 802.2/LLC).

It is another object of the invention to provide a remote access server which provides user authentication and security features. One aspect of these features is that the server can restrict access to the network on a per-user basis. The remote access server controls a remote user's access to the various network services and resources by locating and utilizing one or more access filters for that remote user. The server ensures that each remote user has a particular set of access filters assigned to him or her every time that remote user makes a remote access connection to the network via the server, even though that remote user may utilize a different remote computer every time a remote access connection is made. The server uses a user identification string, which is entered into the remote computer by the remote user, to retrieve from a server-internal or server-external database the access filters associated with that remote user. The database typically is centrally maintained by a network manager with authority to add and delete remote users and access filters.

The remote access server uses the access filters to control the remote users' access to the network and the services, resources, and devices available thereon. The server typically limits a remote user's network access to one or more network "zones" and/or one or more network devices. Zones are pre-defined groups of

devices on the network, and devices can include computers coupled directly to the local network, various servers (e.g., e-mail, database, etc.) and various other network nodes such as printers and plotters.

Because it has the power to control a remote user's access to the resources of the network, the remote access server can ensure that only certain remote users are allowed access to certain resources of the network, such as only those resources listed in the database. If the server locates an access filter for a remote user which indicates that the remote user should not have access to a particular zone or device, that remote user will not be allowed to communicate with that zone or device regardless of the remote computer used in the attempt to gain access. The remote user will, however, be able to communicate with other non-restricted parts of the network. The network restrictions are done by the remote access server on a per-user basis. The remote access server will identify and use access filters for each remote user which attempts to gain access to the network via the server.

Per-user assignment of access filters is very different from other network restriction techniques such as per-port schemes and per-server schemes. With per-port filter assignment, each port of the server has one or more filters associated therewith and those filters are assigned to whichever remote computer happens to communicate through that port. With per-server filter assignment, the server has one or more filters associated therewith and those filters are assigned to whichever remote computers dial into that server. Both the per-port and per-server schemes, unlike per-user, do not provide a correspondence

between a remote user and a set of access filters. These two other schemes do not, unlike per-user, tie network access restriction to remote user identity. It therefore is not possible with either per-port or per-server to control network access precisely, as it is with per-user which is based on the identity of the remote user.

Other objects, aspects, features, and advantages of the invention will become apparent from the following description and from the claims.

Brief Description of the Drawings

In the drawings, like reference characters generally refer to the same parts throughout the different views. Also, the drawings are not necessarily to scale, emphasis instead generally being placed upon illustrating the principles of the invention.

FIG. 1 is a diagram of a remote access system in which a remote access server according to the invention provides a remote user at a remote computer with access to a local computer network.

FIG. 2 is a diagram of a remote access system shown in more detail than the system shown in FIG. 1.

FIG. 3 is a flowchart of the steps a remote access server performs in order to provide a remote user at a remote computer with access to a local computer network according to the invention.

FIG. 4 is a block diagram showing major components of a remote access server according to the invention.

Description

Referring to FIG. 1, in a remote access system 10, a remote computer 12 is allowed access to a local computer network 14 by a remote access server 16. As will be described in more detail later with reference to FIG. 4, the remote access server 16 is itself a powerful programmable computer. In the disclosed embodiment, the remote access server 16 is a LanRover which is available from Shiva Corporation of Burlington, MA. A remote user 18 at the remote computer 12 initiates an attempt to gain access to the network 14 (and the network services and resources available thereon) via the remote access server 16 by entering a user identification (ID) string 20 into the remote computer 12. The user ID string is a pre-determined code which uniquely identifies the remote user, and it typically is assigned to the remote user by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof.

The user ID string 20 entered by the remote user 18 is sent by the remote computer 12 to the remote access server 16 over telephone lines 22. The term telephone lines 22 is used herein to mean any digital and/or analog communication link or links used to transmit voice and/or data including wireless and cellular data links such as Cellular Digital Packet Data (CDPD). In the disclosed embodiment, a modem 24 is connected to the remote computer 12, and another modem 26 is connected to the remote access server 16. The modems 24, 26 allow the remote computer 12 and the remote access server 16 to communicate over the telephone lines 22. Note that the modem 26 connected to the remote access server 16 could be part of the

server 16 (e.g., included within the server housing), as indicated by the dotted-line box 28 enclosing the server 16 and the modem 26 connected thereto. Also note that the modems 24, 26 could be Integrated Services Digital Network (ISDN) terminal adapters if the telephone lines 22 are the ISDN, or the modems 24, 26 could be any of a variety of other switched-access devices.

The remote access server 16 receives the user ID string 20 which was entered by the remote user 18 and sent by the remote computer 12. An optional user authentication procedure may occur at this time where a remote user proves his or her identity by entering a password, by reference to an authentication server database, or by any other method. Once the remote user is authenticated, that remote user is granted access to the network. Further authorization may occur in order for an authenticated user to become an authorized user and be granted access to specific network services. In any event, the server 16 uses the user ID string 20 to index into a database 30 and retrieve one or more access filters associated with the user ID string 20. The server 16 uses these access filters to control the remote user's access to the network 14 and the network services and resources available thereon. The database 30 can be resident in the remote access server 16, or it can be maintained on a node (e.g., a database server) on the network 14. The database 30 includes a unique user ID string for each remote user and at least one access filter for each user ID string. The database 30 typically is maintained by a network manager who has central control of and responsibility for the network 14 and the maintenance thereof. The network manager generally controls (e.g., has the

authority and ability to define, add, and delete) remote user names and access filters.

After the remote access server 16 identifies the access filters for this remote user based on the user ID string 20, the server 16 uses the filters to limit the remote user's network access. Every time the remote computer 12 attempts to communicate on the network 14 via the remote access server 16, the server 16 uses the access filters for that remote user to prevent the remote user from communicating with whatever network resources the filters indicate are off-limits to that remote user.

An access filter can be data packets or words which identify particular network resources such as zones or devices. A zone is a pre-defined group of devices on the network 14. A network device can include computers coupled directly to the local network 14, various servers (e.g., e-mail, database, etc.) coupled directly to the local network 14, and various other nodes on the network 14 such as printers and plotters. Whatever the network resource or resources identified in the access filter, the filter is used by the server 16 to prevent the remote user's remote computer 12 from communicating with the resource(s). Because the database 30 contains a particular set of access filters for certain remote users, the server 16 is able to match one or more filters to each access attempt by those remote users and to limit the network access of those remote users if the filters so dictate.

Filters are protocol dependent and generally employ a look-up service that functions in the following manner. Various network services advertise their presence on the network. Requests for access to network services are processed by the remote access

server. The remote access server refers to another network server that contains an access list. If the user is identified as authorized by the access list, access is granted, otherwise services are simply not identified as being available to the requesting user.

In general, the remote access server 16 will not restrict network access unless the user ID string 20 entered by the remote user 18 at the remote computer 12 corresponds to one or more access filters in the database 30. That is, if the remote access server 16 searches the database 30 but fails to find any access filters associated with the user ID string 20 which the remote user 18 entered at the remote computer 12 (because, for example, the user ID string 20 is in the database 30 but there is no associated access filters listed in the database 30), the remote access server 16 will not limit the network access for that remote user, and thus that remote user will be able to communicate freely on the network 14. In this situation, the remote access server 16 will pass all data packets from the remote computer 12 or the remote user 18 on to the network 14.

The remote access server 16 ensures that each remote user 18 whose network access should be restricted as indicated by the access filters in the database 30 is in fact so restricted every time that remote user 18 makes a remote access connection to the network 14 via the server 16, even though that remote user 18 may utilize a different remote computer 12 every time a remote access connection is made. By linking network access to the identity of the individual remote users, the remote access server 16 can effectively restrict remote users' network access to only those network resources authorized by a central

controller (i.e., the network manager who maintains the database 30).

The remote access system 10 shown generally in FIG. 1 is shown in more detail in FIG. 2. Referring to FIG. 2, the remote computer 12 is a portable laptop computer. In general, the remote computer 12 can be any type of portable computer (e.g., a laptop or a notebook), workstation, or personal computer (e.g., an IBM PC or compatible, an Apple Macintosh, or a Unix-based computer). The remote computer 12 generally must be able to function as a stand-alone computer system when not connected to a network, and as a full network node when it is dialed-in to the network 14 through the remote access server 16. For a remote Macintosh system, it generally is preferred that the computer have a 25 MHz 68030 processor. For a remote PC system, it generally is preferred that the computer have at least a 25 MHz 486 processor.

The remote access system 10 described herein is not to be confused with a remote control system. In a remote control system, a remote user dials-in to the local network with his or her remote computer and takes control of a local computer on the network. Once the remote user's remote computer is connected to the local network in a remote control system, the remote user actually uses the local computer, not the remote computer. That is, only user-interface data (e.g., screen images and keyboard/mouse input) are transferred to the remote computer from the local computer; the remote computer acts as a dumb terminal in a remote control system.

A remote control system is very different from the remote access system 10. In the remote access system 10, the remote computer 12 must perform

adequately by itself, with enough processing power, memory, and disk storage space to run (on the remote computer 12 itself) the remote user's chosen applications without relying upon the on-network communication speed which typically is much higher than the speed of the telephone line link 22. Some telephone lines 22 allow speeds of up to 28.8 kilobits per second whereas the local computer network 14 can operate in ranges from 1 to 100 megabits per second depending on the type of network. The local computer network 14 can be, for example, Ethernet or Token Ring.

The remote computer 12 typically will have a serial port 32 which is managed by a serial controller such as a 16550A serial controller chip which can receive or transmit up to sixteen characters without intervention from the central processing unit (CPU) of the remote computer 12. The modem 24 connected to the serial port 32 can be, for example, a 2400 bits per second or faster Hayes or Hayes compatible modem. A rate of 9600 bits per second or above is recommended for the modem 24. The modem 24 also can be, for example, a V.32bis modem (14.4 kilobits per second) or an ISDN terminal adapter. The other modem 26 (which is not shown in FIG. 2 because it is internal to the remote access server 16) is selected to operate properly given the telephone lines 22 employed and the modem 24 connected to the serial port 32.

The network services and resources available on the network 14 which the remote user 18 might access via the remote access server 16 can include, for example, a Notes Server 46, an E-Mail Server 48, and a Database Server 50. The Database Server 50 can be used to maintain the database 30 of user names and access filters which was described previously with reference

to FIG. 1.

The remote computer 12 can be loaded with network application software 34 and remote access client software 36. The remote access client software 36 can allow, for example, a Macintosh computer to use AppleTalk Remote Access (ARA), a Unix-based computer to use a Point-to-Point Protocol (PPP) implementation, and a PC-based computer to use any standard (if any) or vendor-supplied remote access clients. Briefly, a remote access client includes a "dialer" which establishes and terminates the remote access connection and a "driver" which interfaces with the network. protocol stacks and the serial port 32 to send and receive network data. The remote access client can operate with a variety of protocols including IPX, TCP/IP, NetBEUI, LLC/802.2, and AppleTalk. Novell's IPX is the native protocol for NetWare. TCP/IP is widely used in Unix-based systems and client-server databases, and TCP/IP also is becoming standard for many other applications. NetBEUI is used for LAN Manager and Microsoft's Windows for Workgroups. LLC/802.2 is for IBM LAN Server and host connectivity. The combination of AppleTalk and TCP/IP covers almost all Macintosh applications.

The performance of the remote access server 16 is primarily determined by the ability to move data through its serial ports (shown in FIG. 4 but not in FIG. 2) without much attention from its CPU (also shown in FIG. 4 but not in FIG. 2). The performance of the server 16 also is determined by its CPU's ability to perform the routing, filtering, IP address tracking, etc. that the CPU must do without adding undue delays as it forwards data packets. The server 16 thus has generally been optimized for serial port throughput and

general CPU power. Because the server 16 must be highly reliable and efficient, it includes solid-state, non-volatile storage for the controlling software. The software is upgradeable via downloading from the network 14 to the server 16. The network manager can perform any upgrades.

The software in the remote access server 16 causes the server 16 to perform the various functions described herein, although it should be noted that it is possible to use dedicated electronic hardware to perform all server functionality described herein. The steps which the server performs in order to control a remote user's access to a local computer network according to the invention are shown in FIG. 3.

Referring to FIG. 3, it is first necessary to set-up the connections by coupling a communication port of the remote access server to the telephone lines (step 52) and coupling a network port of the remote access server to the local computer network (step 54). The server is now ready to receive a dial-in from a remote computer over the telephone lines and to communicate on the local network. After the remote access server is set-up, the remote user can cause the remote computer to dial-in and connect to the server over the telephone lines. The remote user then enters into the remote computer a user ID string which the remote computer sends to the server over the telephone lines. The user ID string uniquely identifies that remote user. The remote access server receives the user ID string from the communication port (step 56). Note that after step 56, an optional user authentication procedure may occur where a remote user proves his or her identity by entering a password, by reference to an authentication server database, or by

any other method. Once the remote user is authenticated, that remote user is granted access to teh network. Further authorization may occur in order for an authenticated user to become an authorized user and be granted access to specific network services. In any event, the remote access server then uses the received user ID string to perform a look-up in the database of user ID strings and access filters (step 58). The remote access server retrieves from the database one or more access filters associated with the user ID string, if any (step 60). The remote access server then allows the remote computer to access the local computer network and to communicate on the network, but the server uses the access filter(s) to prevent the remote computer from communicating with the network resource(s) identified by the access filter(s) associated with this remote user (step 62).

Table 1 below shows the database. A variety of other configurations can be employed for the database. Also, the database can include different and/or additional parameters.

USER ID 1	PASSWORD 1	FILTER(S) 1
USER ID 2	PASSWORD 2	FILTER(S) 2
USER ID 3	PASSWORD 3	FILTER(S) 3
.	.	.
.	.	.
.	.	.
USER ID N	PASSWORD N	FILTER(S) N

TABLE 1 - Remote User Information Database

Table 2 below shows an access filter for use in the

remote access system according to the invention. Other configurations of the access filter can be employed. Also, the access filter can include different and/or additional fields. As stated previously, access filters are protocol dependent. As shown in Table 2, a Name Binding Protocol (NBP) Filter includes a Show/Hide (S/H) field, and NBP name field, and a NBP type field.

S/H	NBP Name	NBP Type

TABLE 2 - NBP Filter

As shown in Table 3, a Zone Filter includes an S/H field and a Zone field.

S/H	Zone

TABLE 2 - Zone Filter

Referring now to FIG. 4, in one embodiment, the remote access server 16 includes electronics 38, a plurality of serial communication ports 40_1-40_N, and a plurality of network ports 42_1-42_N. The server 16 also can include a plurality of internal modems 44_1-44_N. The serial ports 40 and the network ports 42 are controlled by the electronics 38.

The electronics 38 include, in some embodiments, a powerful 16 MHz 68EC020 microprocessor and memory such as up to 1 megabyte of battery backed-up static random access memory (SRAM) and possibly 64 kilobytes in an erasable programmable read only memory (EPROM).

Each of the serial communication ports 40 is for

coupling with a communication device (e.g., the modem 26 of FIG. 1), or for coupling directly with the telephone lines 22, to provide for communication with a remote computer (e.g., the remote computer 12 of FIGS. 1 and 2) over the telephone lines 22. A connecting cable can be used to couple a serial port 40 with the communication device or with the telephone lines. Each of the serial ports 40 can simultaneously be coupled to a different one of the plurality of remote computers so as to provide simultaneous access to a local computer network for each of the remote computers, even if each of the remote computers employs a different protocol (e.g., IPX, TCP/IP, AppleTalk, NetBEUI, or 802.2/LLC). In some embodiments, the server 16 includes either four or eight serial ports 40, and each port 40 is a DB-25 asynchronous serial port which supports speeds of up to 57.6 kilobits per second (kbps). In some other embodiments, the server 16 includes four 57.6 kbps ports 40 with an internal V.32bis modem 44 associated with each, and four high-speed (115.2 kbps) serial ports 40 with no internal modem associated therewith. In some other embodiments, the server 16 includes a single port 40 for use with ARA.

Each of the network ports 42 is for coupling with a local computer network (e.g., the network 14 of FIGS. 1 and 2), via a connecting cable, to provide for communication with the network. Typically, the server 16 is connected to only one network during normal operation. In some embodiments, the server 16 includes three network ports 42, one for 10BaseT Ethernet, one for Thin Ethernet, and one for Thick Ethernet. In some other embodiments, the server 16 includes a single network port 42 for Token Ring. In some other embodiments, the server 16 includes a single

network port 42 for use with Apple LocalTalk.

The remote access server 16 shown functionally in FIG. 4 can be contained in a housing similar to that shown in FIG. 2. The housing is less than or equal to about 1.7 by 17 by 10 inches. The housing can be made rack-mountable.

Other modifications and implementations will occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the following claims.

What is claimed is:

Claims

1. A method for limiting access to a local computer network, comprising:

receiving a user identification string from a communication port, the string having been entered by a remote user at a remote computer which is coupled to the communication port, the string identifying the remote user;

using the user identification string to access a database and determine at least one access filter associated with the user identification string, the access filter for preventing the remote computer from communicating with at least one predetermined resource on a local computer network, the database including a user identification string for each remote user and at least one access filter for each user identification string;

allowing the remote computer to access the local computer network and to communicate on the local computer network; and

using the access filter to prevent the remote computer from communicating with the predetermined resource on the local computer network.

2. The method of claim 1 further comprising maintaining the database.

3. The method of claim 1 further comprising coupling a communication device to the communication port for communicating with the remote computer.

4. The method of claim 3 wherein the communication port is a serial port.

5. The method of claim 4 wherein the communication device is a modem.

6. A method for limiting access to a local computer network, comprising:

providing a communication port to provide for communication with a remote computer;

coupling a network port to a local computer network to provide for communication with the local computer network;

receiving a user identification string from the communication port, the string having been entered by a remote user at a remote computer which is coupled to the communication port, the string identifying the remote user;

using the user identification string to access a database and determine at least one access filter associated with the user identification string, the access filter for preventing the remote computer from communicating with at least one predetermined resource on a local computer network, the database including a user identification string for each remote user and at least one access filter for each user identification string;

allowing the remote computer to access the local computer network and to communicate on the local computer network; and

using the access filter to prevent the remote computer from communicating with the predetermined resource on the local computer network.

7. The method of claim 6 further comprising coupling a plurality of communication ports such that a

plurality of remote computers are provided simultaneous limited access to the local computer network.

8. The method of claim 6 further comprising maintaining the database.

9. The method of claim 6 further comprising coupling a communication device to the communication port for communicating with the remote computer.

10. The method of claim 9 wherein the communication port is a serial port.

11. The method of claim 10 wherein the communication device is a modem.

12. A server for limiting access to a local computer network, comprising:
at least one communication port to provide for communication with a remote computer;
at least one network port for coupling to a local computer network to provide for communication with the local computer network; and
processing electronics for:
controlling the communication port and the network port,
receiving from the communication port a user identification string which was entered by a remote user at a remote computer and which identifies the remote user,
using the user identification string to access a database and determine at least one access filter associated with the user identification string, the access filter for preventing the remote computer from

communicating with at least one predetermined resource on the local computer network, the database including a user identification string for each remote user and at least one access filter for each user identification string,

allowing the remote computer to access the local computer network and to communicate on the local computer network, and

using the access filter to prevent the remote computer from communicating with the predetermined resource on the local computer network.

13. The server of claim 12 further comprising a plurality of communication ports such that a plurality of remote computers are provided simultaneous access to the local computer network through the server.

14. The server of claim 12 wherein the processing electronics includes a microprocessor and memory.

15. The server of claim 12 wherein the database is maintained internally by the server.

16. The server of claim 12 wherein the database is maintained on the local computer network and external from the server.

17. The server of claim 12 further comprising a communication device coupled to the communication port for communicating with the remote computer.

18. The server of claim 17 wherein the communication port is a serial port.

19. The server of claim 18 wherein the communication device is a modem.

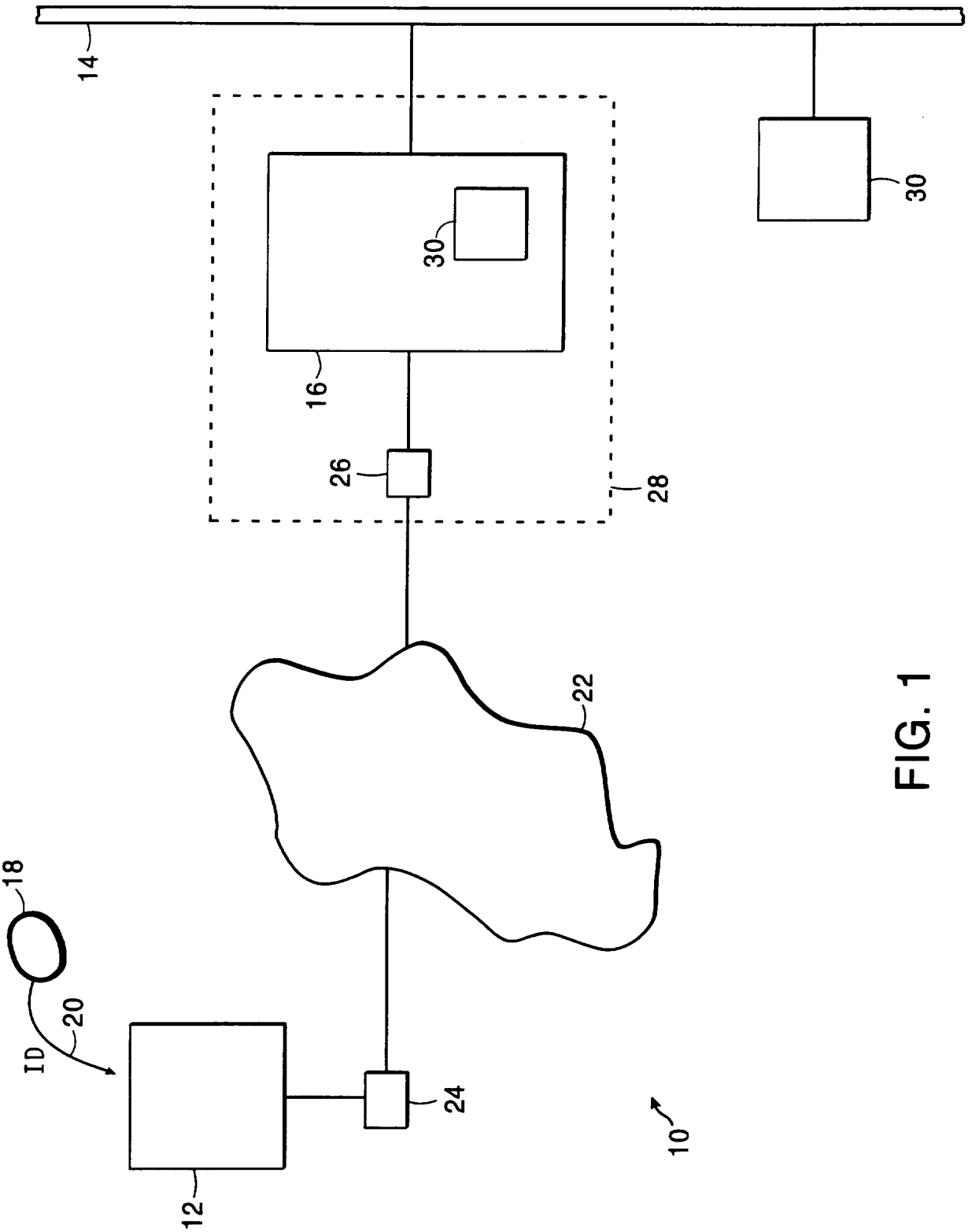

FIG. 1

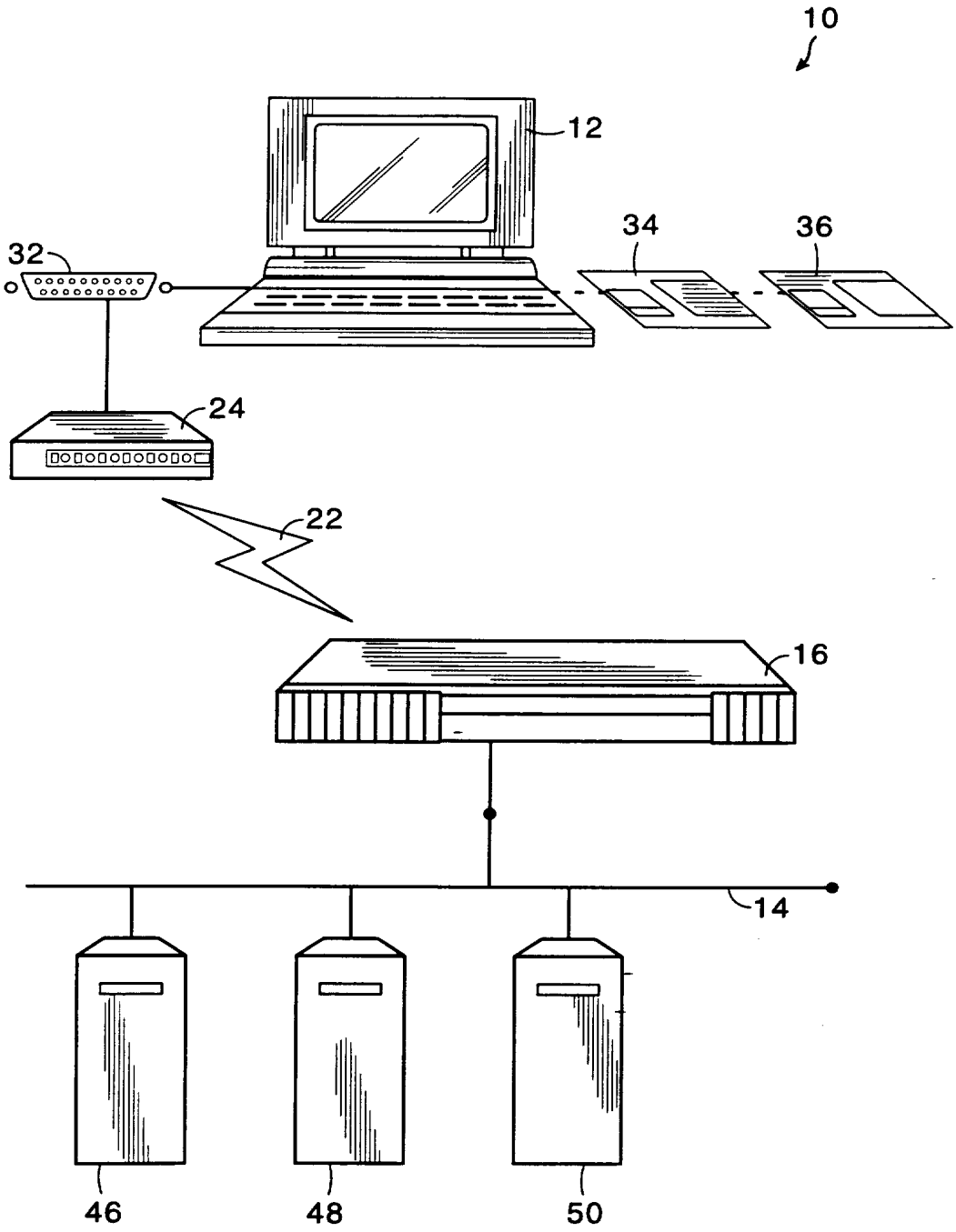

FIG. 2

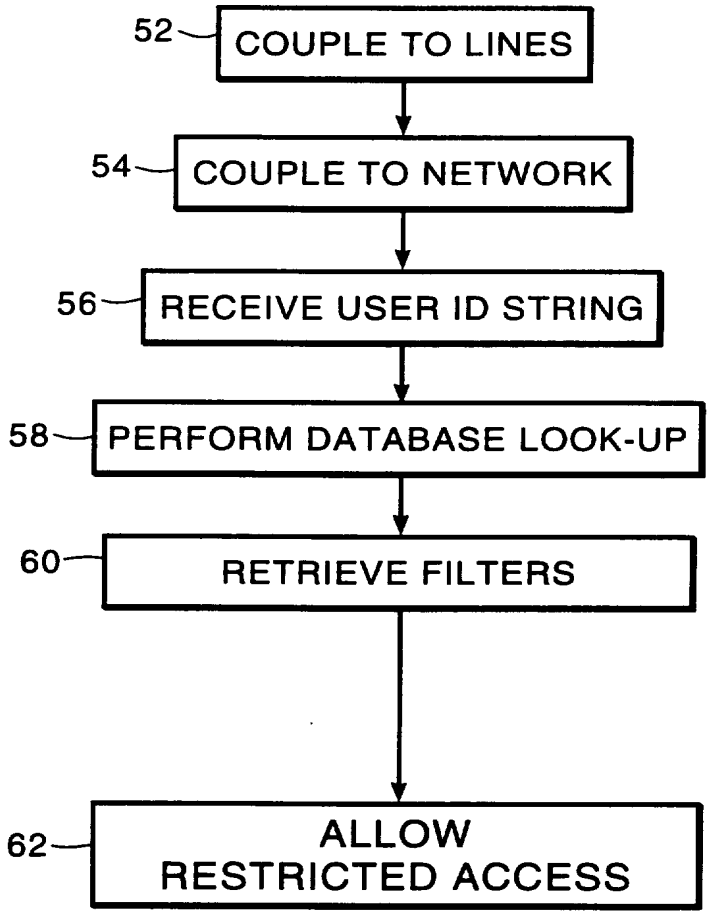
52
COUPLE TO LINES
54
COUPLE TO NETWORK
56
RECEIVE USER ID STRING
58
PERFORM DATABASE LOOK-UP
60
RETRIEVE FILTERS
62
ALLOW
RESTRICTED ACCESS

FIG. 3

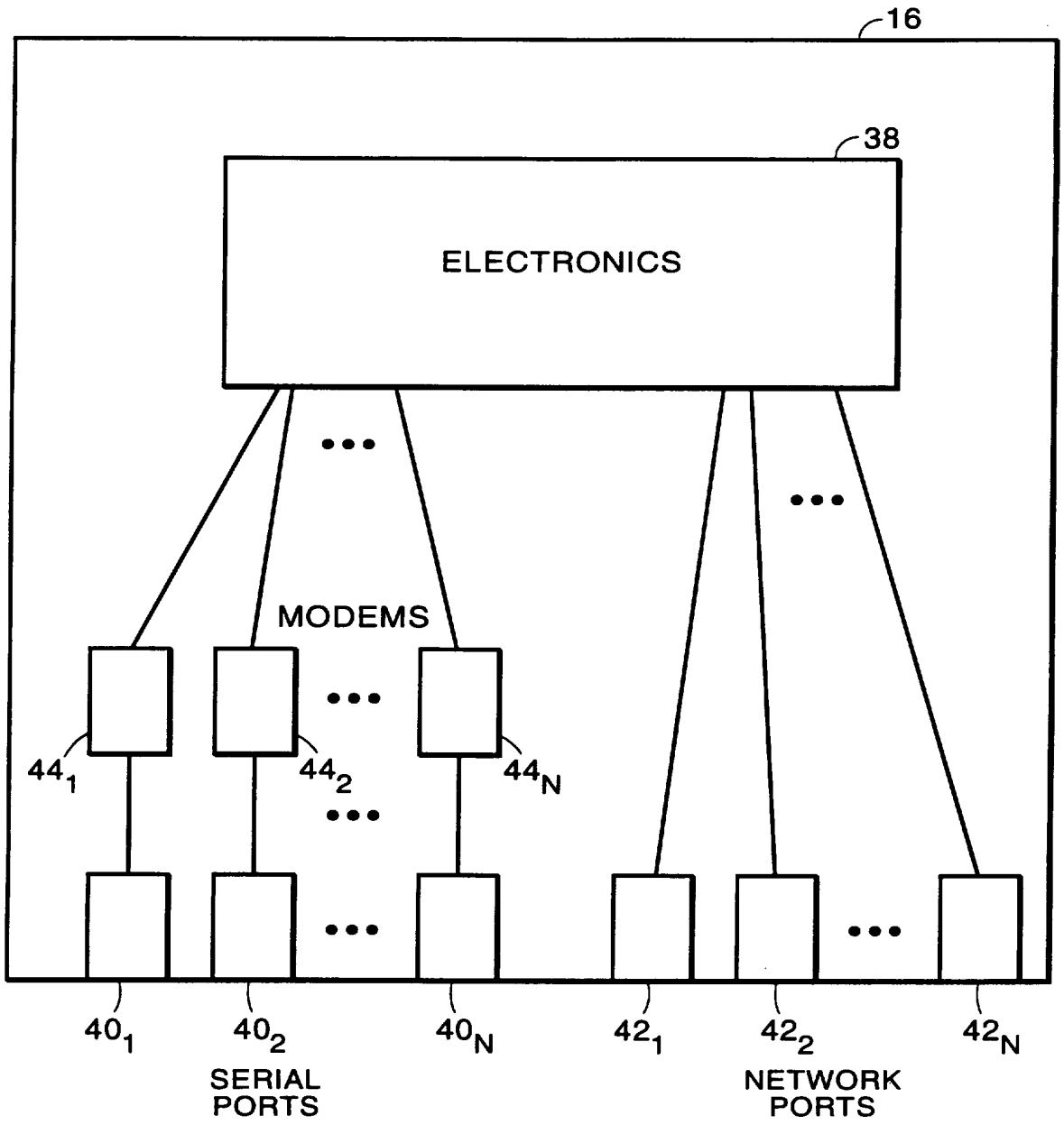
16
38
ELECTRONICS
MODEMS
44_1
44_2
44_N
40_1
40_2
40_N
42_1
42_2
42_N
SERIAL PORTS
NETWORK PORTS

FIG. 4

INTERNATIONAL SEARCH REPORT

Inte. .onal Application No
PCT/US 95/08900

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP,A,0 513 484 (BULL HN INFO. SYSTEMS) 19 November 1992 see abstract; figures 1-3 see column 3, line 51 - column 4, line 15 see column 5, line 3 - line 50 ---	1-12,14, 15,17-19
Y	INTERNATIONAL CONF. ON ENERGY, COMPUTER, COMMUNICATION AND CONTROL SYSTEMS, 30 August 1991, NEW DELHI, INDIA; pages 103 - 107 S.K.BOSE ET AL 'Remote DOS Disk Server on a UNIX Machine' see abstract; figure 4 see page 105, left column, line 7 - line 46 see page 106, left column, line 62 - page 107, left column, line 12 --- -/--	1-12,14, 15,17-19

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
17 November 1995	27.12.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte. ational Application No
PCT/US 95/08900

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,4 310 720 (CHECK, JR.) 12 January 1982 see abstract; figure 1	4,5, 10-12, 14,15, 17-19

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter onal Application No
PCT/US 95/08900

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0513484	19-11-92	AU-B-	1135392	24-09-92
US-A-4310720	12-01-82	CA-A-	1102453	02-06-81
		DE-A-	2912696	11-10-79
		FR-A,B	2421426	26-10-79
		GB-A,B	2019060	24-10-79
		GB-A,B	2076615	02-12-81
		JP-A-	54136205	23-10-79